# La CJUE invalide le Safe Harbor



## Qu’est-ce que le Safe Harbor ?

Le « Safe Harbor » (en français sphère de sécurité) est un ensemble de principes de protection des données personnelles, publié par le Département du Commerce américain, auxquels des entreprises établies aux Etats-Unis adhèrent afin de pouvoir recevoir des données en provenance de l’Union européenne. Ces principes, négociés entre les autorités américaines et la Commission européenne, sont essentiellement basés sur ceux de la Directive européenne 95/46 du 24 octobre 1995. Le 26 juillet 2000, la Commission Européenne a adopté une décision d’adéquation qui reconnaît que les principes de « Safe Harbor » assurent une protection adéquate pour les besoins des transferts de données à caractère personnel depuis l’Union Européenne. En conséquence, le transfert des données personnelles de l’UE vers les USA est légal dès lors que l’entreprise américaine est certifiée. La liste des entreprises certifiée (U.S.-EU SAFE HARBOR LIST) est disponible sur le site du département du commerce américain et recense à l’heure actuelle 5482 sociétés.

## Pourquoi cet accord était-il fortement critiqué ?

Tout a commencé avec le Patriot Act., la loi anti-terroriste promulguée le 26 octobre 2001 en réponse aux attentats du 11 septembre. En donnant de très larges pouvoirs aux services de renseignement avec les NSL (National Security Letters) via une législation dérogatoire, le Safe Harbor ne pouvait plus garantir la confidentialité des données hébergées auprès de sociétés de droit américain ou de leurs filiales. En juin 2013, les révélations d’Edward Snowden n’ont fait que confirmer les programmes (PRISM, Xkeyscore,…) d’espionnage de masse des européens avec la collaboration active des leaders américains de l’Internet (Facebook, Microsoft, Apple,…). Si les européens avaient bien connaissance des lois (FISA, Patriot Act) qui permettent aux autorités américaines d’accéder à leurs données personnelles pour assurer la sécurité nationale du pays, ils n’imaginaient pas que les Américains s’en serviraient pour établir une surveillance à des fins économiques et géopolitiques. D’autre part, le secret autour des activités des services de renseignement relevant du gouvernement américain empêche toute vérification du

respect des principes de la Directive Européenne (95/46) notamment sur les activités de recueil, de traitement, de conservation des données et empêche tout contrôle des intéressés sur ces activités.

Pour sa certification l'entreprise américaine peut faire appel à un tiers ou contrôler elle-même qu'elle se conforme aux exigences du Safe Harbor. C'est donc le principe de l'auto-évaluation (self-assessment) qui sera retenue par la plupart des entreprises américaines. Même si l'entreprise doit renouveler sa certification chaque année (selon le même principe), il apparait clairement que de nombreuses sociétés inscrites sur la liste des entreprises certifiée n'ont fait que s'auto-proclamer « Safe Harbor Compliant » en ne respectant en aucune manière les exigences réelles du Safe Harbor. D'autre part, le contrôle du programme étant exclusivement assuré par la Federal Trade Commission, les CNIL européennes (G29) n'ont aucun moyen de contrôler (et encore moins de sanctionner) les entreprises américaines contrevenantes.

## Pourquoi la CJUE a-t-elle été saisie ?

L'affaire démarre en 2011 lorsque un jeune étudiant autrichien de 24 ans, Maximilian Schrems, reproche à Facebook de violer les lois européennes sur la protection des données personnelles. Dans un entretien à Pixels en août 2014, Max Schrems déclare :

« J'assistais à une conférence aux Etats-Unis  et quelqu'un de Facebook est venu nous expliquer comment les lois européennes sur la vie privée fonctionnaient. J'étais le seul Européen. Et il disait : "Vous pouvez faire ce que vous voulez, rien ne vous arrivera jamais". Il interprétait la loi européenne d'une façon qui était complètement fausse. Il disait des choses comme : "*Tant que personne ne vous dit non, vous po*uvez continuer à utiliser l*eurs données".* »

*Max Schrems en janvier 2012. DIETER NAGL / AFP*

Il décide alors de porter plainte contre Facebook à Dublin là où se situe le siège européen du géant américain. En première instance, la justice irlandaise rejette sa demande en considérant que le transfert des données vers les datacenters américains de Facebook étaient couverts par le Safe Harbor. Devenu avocat, et suite aux révélations de Snowden en juin 2013, Schrems ne lâche pas l'affaire et décide de faire appel. Pour prendre sa décision, la High Court of Ireland (Haute Cour de justice irlandaise) demande alors l'avis de la CJUE pour statuer sur cette affaire.

## Quelles sont les motivations de la CJUE ?

La CJUE a désigné, Yves Bot, avocat général, pour instruire cette affaire. Par décision du Conseil européen, la CJUE dispose aujourd'hui de 11 avocats généraux et selon l'article 252 du Traité sur le fonctionnement de l'Union européenne :
« L'avocat général a pour rôle de présenter publiquement, en toute impartialité et en toute indépendance, des conclusions motivées sur les affaires qui, conformément au statut de la Cour de justice de l'Union européenne, requièrent son intervention. »

Dans ses conclusions, rendues publiques le 23 septembre 2015, Yves Bot étudie plusieurs questions fondamentales auxquelles il apporte les réponses suivantes :

- Quel est le rôle et quelles sont les capacités d'une autorité de régulation nationale face aux accords européens comme le *Safe Harbor* ? Peut-elle enquêter et agir contre des entreprises couvertes par ce type d'accord ?

*Une autorité nationale de protection des données a le droit et le devoir de défendre*

*les citoyens même en présence d'un accord européen*

- Que se passe-t-il lorsqu'un accord passé il y a 15 ans (le *Safe Harbor* est en vigueur depuis 2000) n'est pas révisé alors qu'il a été porté à la connaissance du public que des traitements de données personnelles ont été effectués en dehors des finalités prévues par cet accord ?

*La Commission européenne devait vérifier périodiquement la conformité du Safe Harbor aux standards de protection des données européens*

- Peut-on considérer que l'accès aux données des européens par les services de renseignement américains respecte les principes de proportionnalité et de finalités explicites qui sont jugés nécessaires au respect des droits fondamentaux en Europe, y compris lorsque sont invoqués les motifs de sécurité nationale ?

*Les conditions de respect des principes de proportionnalité et de finalités explicites ne sont pas respectés par les services de renseignement américains*

- Comment faire respecter les droits des citoyens européens lorsqu'il n'existe pas de possibilité de recours juridictionnel respectant les standards européens dans le pays qui reçoivent leurs données personnelles ?

Les citoyens européens ne disposent pas des garanties nécessaires à l'exercice de leurs droits contre le traitement de leurs données par les services de renseignement

- La Commission européenne aurait-elle dû d'elle-même suspendre le transfert des données personnelles ou au moins réviser périodiquement le *Safe Harbor* afin de vérifier que les critères de conformité prévus à l'origine continuaient d'être respectés ?

*Oui en conséquence, le Safe Harbor doit être invalidé et suspendu*

Les conclusions de l'avocat général de la CJUE étant consultatives, il faudra attendre le 6 octobre 2015 pour que la CJUE rende son jugement définitif en déclarant invalide la décision 2000/520 de la Commission du 26 juillet 2000 instaurant le principe de « Safe Harbor ».

Dans son communiqué de Presse , La CJUE indique :

« *Pour toutes ces raisons, la Cour déclare la décision de la Commission du 26 juillet 2000 invalide. Cet arrêt a pour conséquence que l'autorité irlandaise de*

*contrôle est tenue d'examiner la plainte de M. Schrems avec toute la diligence requise et qu'il lui appartient, au terme de son enquête, de décider s'il convient, en vertu de la directive, de suspendre le transfert des données des abonnés européens de Facebook vers les États-Unis au motif que ce pays n'offre pas un niveau de protection adéquat des données personnelles.* »

## Que va-t-il se passer maintenant ?

Tout d'abord, l'autorité de contrôle irlandaise va devoir mener des investigations et prendre une décision concernant l'affaire Schrems/Facebook. Mais au-delà de cette affaire, il s'ouvre une période d'incertitude juridique pour tous les acteurs (fournisseurs américains et client européens). Des clarifications rapides sont attendues de la part de la commission européenne mais également du groupe de travail des CNIL européennes (G29). Dans ce contexte, il est fort probable qu'un Safe Harbor v2 voit le jour rapidement pour prendre en compte les exigences européennes.

Dans l'immédiat, il est fortement recommandé aux entreprises de procéder à un audit afin de répertorier tous les traitements de données personnelles dont le transfert s'est appuyé sur la base juridique du Safe Harbor. Notons pour finir qu'il existe d'autres possibilités pour transférer légalement des données personnelles vers les états-unis : les Binding Corporate Rules (BCR), les clauses contractuelles types (CCT) ou encore, lorsque c'est possible, les exceptions à l'interdiction des flux transfrontières visées à l'article 69 de la loi Informatique et libertés.